CHAPTER

Domain 1: Security risk management

1

CHAPTER OUTLINE

Eleventh Hour CISSP®. http://dx.doi.org/10.1016/B978-0-12-811248-9.00001-2

INTRODUCTION

Our job as information security professionals is to evaluate *risks* against our critical *assets* and deploy *safeguards* to mitigate those risks. We work in various roles: firewall engineers, penetration testers, auditors, management, etc. The common thread is risk, which is part of our job description.

The Security and Risk Management domain focuses on risk analysis and mitigation. This domain also details security governance, or the organizational structure required for a successful information security program. The difference between organizations that are successful versus those that fail in this realm is usually not tied to budget or staff size; rather, it is tied to the right people in the right roles. Knowledgeable and experienced information security staff with supportive and vested leadership is the key to success.

Speaking of leadership, learning to speak the language of your leadership is another key to personal success in this industry. The ability to effectively communicate information security concepts with C-level executives is a rare and needed skill. This domain will also help you to speak their language by discussing risk in terms such as *total cost of ownership (TCO)* and *return on investment (ROI)*.

CORNERSTONE INFORMATION SECURITY CONCEPTS

Before we can explain access control, we must define cornerstone information security concepts. These concepts provide the foundation upon which the eight domains of the Common Body of Knowledge are built.

CONFIDENTIALITY, INTEGRITY, AND AVAILABILITY

Confidentiality, *integrity*, and *availability* are referred to as the CIA triad, which is the cornerstone concept of information security. The triad, shown in Fig. 1.1, forms the three-legged stool upon which information security is built. The order of the acronym may change (some prefer AIC, perhaps to avoid association with a certain intelligence agency), but that is not important; what is critical is understanding each concept. This book will use the CIA acronym.

Confidentiality

Confidentiality seeks to prevent the unauthorized disclosure of information; it keeps data secret. In other words, confidentiality seeks to prevent unauthorized read access to data. An example of a confidentiality attack would be the theft of *personally identifiable information* (PII), such as credit card information.

Integrity

Integrity seeks to prevent unauthorized modification of information. In other words, integrity seeks to prevent unauthorized write access to data.

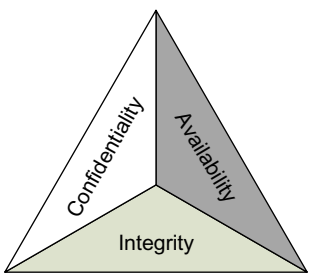

FIG. 1.1

The CIA triad.

CRUNCH TIME

There are two types of integrity: data integrity and system integrity. Data integrity seeks to protect information from unauthorized modification, while system integrity seeks to protect a system, such as a Windows 2012 server operating system, from unauthorized modification.

Availability

Availability ensures that information is available when needed. Systems need to be usable (available) for normal business use. An example of attack on availability would be a *denial of service* (DoS) attack, which seeks to deny service (or availability) of a system.

Disclosure, alteration, and destruction

The CIA triad may also be described by its opposite: *disclosure, alteration, and destruction* (DAD). Disclosure is the unauthorized release of information, alteration is the unauthorized modification of data, and destruction is making systems or data unavailable. While the order of the individual components of the CIA acronym sometimes changes, the DAD acronym is shown in that order.

IDENTITY AND AUTHENTICATION, AUTHORIZATION, AND ACCOUNTABILITY

The term AAA is often used to describe the cornerstone concepts *authentication, authorization, and accountability*. Left out of the AAA acronym is *identification*, which is required before the remaining three As can be achieved.

Identity and authentication

Identity is a claim: If your name is "Person X," you identify yourself by saying, "I am Person X." Identity alone is weak because there is no proof. You can also identify yourself by saying, "I am Person Y." Proving an identity claim is called authentication. You authenticate the identity claim, usually by supplying a piece of information or an object that only you possess, such as a password or your passport.

Authorization

Authorization describes the actions you can perform on a system once you have been identified and authenticated. Actions may include reading, writing, or executing files or programs.

Accountability

Accountability holds users accountable for their actions. This is typically done by logging and analyzing audit data. Enforcing accountability helps keep honest people honest. For some users, knowing that data is logged is not enough to provide

accountability; they must know that the data is logged and audited, and that *sanctions* may result from violation of *policy*.

NONREPUDIATION

Nonrepudiation means a user cannot deny (repudiate) having performed a transaction. It combines authentication and integrity; nonrepudiation authenticates the identity of a user who performs a transaction and ensures the integrity of that transaction. You must have both authentication and integrity to have nonrepudiation; for example, proving you signed a contract to buy a car (authenticating your identity as the purchaser) is not useful if the car dealer can change the price from $20,000 to $40,000 (violate the integrity of the contract).

LEAST PRIVILEGE AND NEED TO KNOW

Least privilege means users should be granted the minimum amount of access (authorization) required to do their jobs, but no more. Need to know is more granular than least privilege; the user must need to know that specific piece of information before accessing it.

SUBJECTS AND OBJECTS

A *subject* is an active entity on a data system. Most examples of subjects involve people accessing data files. However, computer programs can be subjects as well. A dynamic link library file or a Perl script that updates database files with new information is also a subject.

An *object* is any passive data within the system. Objects can range from documents on physical paper to database tables to text files. The important thing to remember about objects is that they are passive within the system; they do not manipulate other objects.

DEFENSE IN DEPTH

Defense in depth (also called layered defense) applies multiple safeguards (also called controls, which are measures taken to reduce risk) to protect an asset. Any single security control may fail; by deploying multiple controls, you improve the confidentiality, integrity, and availability of your data.

LEGAL AND REGULATORY ISSUES

Though general understanding of major legal systems and types of law is important, it is critical that information security professionals understand the concepts described in the next section. With the ubiquity of information systems, data, and applications comes a host of legal issues that require attention.

COMPLIANCE WITH LAWS AND REGULATIONS

Complying with laws and regulations is a priority for top information security management, both in the real world and on the exam. An organization must be in compliance with all laws and regulations that apply to it. Ignorance of the law is never a valid excuse for breaking the law.

MAJOR LEGAL SYSTEMS

In order to begin to appreciate common legal concepts at work in today's global economy, an understanding of the major legal systems is required. These legal systems provide the framework that determines how a country develops laws pertaining to information systems in the first place. The three major systems of law are civil, common, and religious law.

Civil law (legal system)

The most common of the major legal systems is that of *civil law*, which is employed by many countries throughout the world. The system of civil law leverages codified laws or statutes to determine what is considered to be within the bounds of law. Though a legislative branch typically wields the power to create laws, there will still exist a judicial branch that is tasked with interpretation of the existing laws. The most significant difference between civil and common law is that under civil law judicial precedents and particular case rulings do not carry the weight they would have under common law.

Common law

Common law is the legal system used in the United States, Canada, the United Kingdom, and most former British colonies, amongst others. As we can see by the short list above, English influence has historically been the main indicator of common law being used in a country. The primary distinguishing feature of common law is the significant emphasis on particular cases and judicial precedents as determinants of laws. Though there is typically also a legislative body tasked with the creation of new statutes and laws, judicial rulings can at times supersede those laws. Because of the emphasis on judges' interpretations, there is significant possibility that as society changes over time, so can judicial interpretations.

Religious and customary law

Religious law serves as the third of the major legal systems. Religious doctrine or interpretation serves as the primary source of legal understanding and statutes. While Christianity, Judaism, and Hinduism have all had significant influence on national legal systems, Islam serves as the most common source for religious legal systems. Sharia is an example of Islamic law that uses the Qur'an and Hadith as its foundation.

Customary law refers to those customs or practices that are so commonly accepted by a group that the custom is treated as a law. These practices can be later codified as laws in the more traditional sense, but the emphasis on the prevailing acceptance of a group is quite important.

CRIMINAL, CIVIL, AND ADMINISTRATIVE LAW

Within common law there are various branches of laws, including criminal, civil, and administrative law.

Criminal law

Criminal law pertains to those laws where the victim can be seen as society itself. While it might seem odd to consider society the victim when an individual is murdered, the goal of criminal law is to promote and maintain an orderly and law-abiding citizenry. Criminal law can include penalties that remove an individual from society by incarceration or, in some extreme cases in some regions, death. The goals of criminal law are to deter crime and to punish offenders.

Due to the severity of depriving criminals of either freedom or their lives, the burden of proof in criminal cases is beyond any reasonable doubt.

Civil law

In addition to *civil law* being a major legal system in the world, it also serves as a type of law within the common law legal system. Another term associated with civil law is tort law, which deals with injury (loosely defined), resulting from someone violating their responsibility to provide a duty of care. Tort law is the primary component of civil law, and it is the most significant source of lawsuits that seek damages.

In the United States, the burden of proof in a criminal court is beyond a reasonable doubt, while the burden of proof in civil proceedings is the preponderance of the evidence. "Preponderance" means more likely than not. Satisfying the burden of proof requirement regarding the preponderance of the evidence in a civil matter is much easier than meeting the burden of proof requirement in criminal proceedings. The most common types of financial damages are presented in Table 1.1.

Administrative law

Administrative law or *regulatory law* is law enacted by government agencies. The executive branch (deriving from the Office of the President) enacts administrative law in the United States. Government-mandated compliance measures are administrative laws. Some examples of administrative law are FCC regulations, Health Insurance Portability and Accountability Act (HIPAA) security mandates, FDA regulations, and FAA regulations.

LIABILITY

Legal liability is another important legal concept for information security professionals and their employers. Society has grown quite litigious over the years, and the question of whether an organization is legally liable for specific actions or inactions can prove costly. Questions of liability often turn into questions regarding potential negligence. When attempting to determine whether certain actions or inactions constitute negligence, the *Prudent Man Rule*, which we will define shortly, is often applied.

Table 1.1 Common Types of Financial Damages

Financial Damages	Description
Statutory	Statutory damages are those prescribed by law, which can be awarded to the victim even if the victim incurred no actual loss or injury
Compensatory	The purpose of compensatory damages is to provide the victim with a financial award in effort to compensate for the loss or injury incurred as a direct result of the wrongdoing
Punitive	The intent of punitive damages is to punish an individual or organization. These damages are typically awarded to attempt to discourage a particularly egregious violation where the compensatory or statutory damages alone would not act as a deterrent

Two important terms to understand are due care and due diligence, which have become common standards that are used in determining corporate liability in courts of law.

DUE CARE AND DUE DILIGENCE

Due care is doing what a reasonable person would do in a given situation. It is sometimes called the "prudent man" rule. The term is derived from "duty of care"; for example, parents have a duty to care for their children. *Due diligence* is the management of due care.

Due care and due diligence are often confused; they are related, but there is a difference between them. Due care is informal, while due diligence follows a process. Think of due diligence as a step beyond due care. For example, expecting your staff to keep their systems patched means that you expect them to exercise due care, while verifying that your staff has patched their systems is an example of due diligence.

Gross negligence

Gross negligence is the opposite of due care. It is a legally important concept. For example, if you suffer loss of PII, but can demonstrate due care in protecting the PII, you are on stronger ground in a legal proceeding. If you cannot demonstrate due care (ie, you acted with gross negligence), you are in a much worse legal position.

LEGAL ASPECTS OF INVESTIGATIONS

Investigations are a critical way in which information security professionals come into contact with the law. Forensic and incident response personnel often conduct investigations, therefore both need to have a basic understanding of legal matters to ensure that the legal merits of the investigation are not unintentionally tarnished.

Evidence

Evidence is one of the most important legal concepts for information security professionals to understand. Information security professionals are commonly involved in investigations, and they often have to obtain or handle evidence during the investigation.

CRUNCH TIME

Real evidence consists of tangible or physical objects. A knife or bloody glove might constitute real evidence in some traditional criminal proceedings. *Direct evidence* is testimony provided by witnesses regarding what they actually experienced through their five senses. *Circumstantial evidence* serves to establish the circumstances related to particular points or other evidence. *Corroborative evidence* provides additional support for a fact that might have been called into question. *Hearsay evidence* constitutes second-hand evidence. As opposed to direct evidence, which is witnessed using any of the five senses, hearsay evidence involves indirect information. *Secondary evidence* consists of copies of original documents and oral descriptions. Computer-generated logs and documents might also constitute secondary rather than best evidence, which we will define shortly.

Best evidence rule

Courts prefer the best evidence possible. Original documents are preferred over copies, and conclusive tangible objects are preferred over oral testimony. The *best evidence rule* prefers evidence that meets these criteria.

Evidence integrity

Evidence must be reliable. It is common during forensic and incident response investigations to analyze digital media. It is critical to maintain the integrity of the data during the course of its acquisition and analysis. Checksums can ensure that no data changes occurred as a result of the acquisition and analysis. One-way hash functions such as MD5 or SHA-1 are commonly used for this purpose. *Chain of custody* requires that once evidence is acquired, full documentation must be maintained regarding who or what handled the evidence and when and where it was handled.

Entrapment and enticement

Entrapment is when law enforcement, or an agent of law enforcement, persuades someone to commit a crime when the person otherwise had no intention to commit a crime. Enticement could still involve agents of law enforcement making the conditions for commission of a crime favorable, but the difference is that the person is determined to have already broken a law or is intent on doing so.

COMPUTER CRIME

One aspect of the interaction of information security and the legal system is that of *computer crimes*. Applicable computer crime laws vary throughout the world, according to jurisdiction. However, regardless of region, some generalities exist.

FAST FACTS

Computer crimes can be based upon the way in which computer systems relate to the wrongdoing. For example, computer systems can be used as targets, or they can be used as the tools used in perpetrating the crime.

Computer systems as target of crime—Examples include disrupting online commerce by means of distributed DoS attacks, installing malware on systems for the distribution of spam, or exploiting vulnerability of a system to store illegal content.

Computer as a tool used to perpetrate crime—Examples include leveraging computers to steal cardholder data from payment systems, conducting computer based reconnaissance to target an individual for information disclosure or espionage, and using computer systems for the purposes of harassment.

INTELLECTUAL PROPERTY

As opposed to physical or tangible property, *intellectual property* refers to intangible property that is created as the result of a creative act. The following intellectual property concepts effectively create an exclusive monopoly on their use.

Trademark

Trademarks are associated with marketing. A trademark allows for the creation of a brand in order to distinguish the source of products or services. A name, logo, symbol, or image represents the most commonly trademarked items. In the United States, there are two different symbols that are used by an individual or organization in order to protect distinctive marks. The superscript TM symbol, as seen in Fig. 1.2, can be used freely to indicate an unregistered mark. The circle R symbol, as seen in Fig. 1.3, is used with marks that have been formally registered as a trademark with the US Patent and Trademark Office.

Patent

Patents provide a monopoly to the patent holder regarding the right to use, make, or sell an invention for a period of time in exchange for the patent holder's promise to make the invention public. During the life of the patent, the patent holder can, through the use of civil litigation, exclude others from leveraging the patented invention. Obviously, in order for an invention to be patented, it should be novel and unique. The patent term, which is the length that a patent is valid, varies by region

Syngress™

FIG. 1.2

Trademark symbol.

Syngress®

FIG. 1.3

Registered trademark symbol.

FIG. 1.4

Copyright symbol.

and also by the type of invention being patented. Generally, in both Europe and the United States, the patent term is 20 years from the initial filing date.

Copyright

Copyright represents a type of intellectual property that protects the form of expression in artistic, musical, or literary works and is typically denoted by the circled c symbol, as shown in Fig. 1.4. The purpose of a copyright is to preclude unauthorized duplication, distribution, or modification of a creative work. Note that it is the form of expression that is protected, not the subject matter or ideas represented.

Licenses

Software licenses are a contract between a provider of software and the consumer. Though there are licenses that provide explicit permission for the consumer to do virtually anything with the software, including modifying it for use in another commercial product, most commercial software licensing provides explicit limits on the use and distribution of the software. Software licenses, such as end-user license agreements (EULAs), are an unusual form of contract because using the software typically constitutes contractual agreement, even though a small minority of users read the lengthy EULA.

Trade secrets

Trade secrets are business-proprietary information that is important to an organization's ability to compete. The organization must exercise due care and due diligence in the protection of their trade secrets. Noncompete and nondisclosure agreements are two of the most common protection methods used.

PRIVACY

Privacy is the protection of the confidentiality of personal information. Many organizations host users' PII such as Social Security numbers, financial information (eg, annual salary and bank account information required for payroll deposits), and health care information for insurance purposes. The confidentiality of this information must be assured.

European union privacy

The European Union has taken an aggressive proprivacy stance while balancing the needs of business. Commerce would be impacted if member nations had different regulations regarding the collection and use of PII. The *EU Data Protection Directive* allows for the free flow of information while still maintaining consistent protection of citizen data in each member nation.

FAST FACTS

The principles of the EU Data Protection Directive are:

- Notifying individuals how their personal data is collected and used
- Allowing individuals to opt out of sharing their personal data with third parties
- Granting individuals the right to choose to opt into sharing the most sensitive personal data, as opposed to being opted in automatically.
- Providing reasonable protections for personal data

OECD privacy guidelines

The Organisation for Economic Co-operation and Development (OECD), though often considered exclusively European, consists of 30 member nations from around the world. The members include such countries as the United States, Mexico, Australia, Japan, and the Czech Republic, as well as prominent European countries. The OECD provides a forum in which countries can focus on issues that impact the global economy. The OECD will routinely issue consensus recommendations that can serve as an impetus to change current policies and legislation in the OECD member countries and beyond.

EU-US safe harbor

An interesting aspect of the EU Data Protection Directive is that the personal data of EU citizens may not be transmitted, even when permitted by the individual, to countries outside of the EU unless the receiving country is perceived by the EU to adequately protect their data. This presents a challenge regarding the sharing of the data with the United States, which is perceived to have less stringent privacy protections. To help resolve this issue, the United States and the European Union created the Safe Harbor framework that will give US-based organizations the benefit of authorized data sharing. In order to participate, US organizations must voluntarily consent to data privacy principles that are consistent with the EU Data Protection Directive.

INTERNATIONAL COOPERATION

To date, the most significant progress toward international cooperation in computer crime policy is the Council of Europe Convention on Cybercrime. In addition to the treaty being signed and subsequently ratified by a majority of the 47 European member countries, the United States has also signed and ratified the treaty. The primary focus of the Convention on Cybercrime is to establish standards in cybercrime policy in order to promote international cooperation during the investigation and prosecution of cybercrime. Additional information on the Council of Europe Convention on Cybercrime can be found here: http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185.

IMPORT/EXPORT RESTRICTIONS

Due to the successes of cryptography, many nations have limited the import and/or export of cryptosystems and associated cryptographic hardware. In some cases, countries would prefer that their citizens be denied the use of any cryptosystems that their intelligence agencies cannot crack, and therefore those countries attempt to impose import restrictions on cryptographic technologies.

During the Cold War, CoCom, the Coordinating Committee for Multilateral Export Controls, was a multinational agreement restricting the export of certain technologies, which included encryption, to many Communist countries. After the Cold War, the Wassenaar Arrangement became the standard for export controls. This multinational agreement was far less restrictive than the former CoCom, but did still suggest significant limitations on the export of cryptographic algorithms and technologies to countries not included in the Wassenaar Arrangement.

SECURITY AND THIRD PARTIES

Organizations are increasingly reliant upon third parties to provide significant and sometimes business-critical services. While leveraging external organizations is by no means a recent phenomenon, the critical nature of their roles and the volume of services and products now typically warrant specific attention toward an organization's information security department.

SERVICE PROVIDER CONTRACTUAL SECURITY

Contracts are the primary control for ensuring security when dealing with services provided by third-party organizations. The tremendous surge in outsourcing, especially the ongoing shift toward cloud services, has made contractual security measures much more prominent.

Service level agreements

Service level agreements (SLA) identify key expectations that the vendor is contractually required to meet. SLAs are widely used for general performance expectations, but are increasingly leveraged for security purposes as well. SLAs primarily address availability.

Attestation

Information security attestation involves having a third-party organization review the practices of the service provider and make a statement about the security posture of the organization. The goal of the service provider is to provide evidence that they can and should be trusted. Typically, a third party provides attestation after performing an audit of the service provider against a known baseline.

Right to penetration test/right to audit

The right to penetration test and right to audit documents provide the originating organization with written approval to perform their own testing or have a trusted provider perform the assessment on their behalf.

An alternative to the right to penetration test/right to audit documents is for the service provider to present the originating organization with a third-party audit or penetration test that the service provider had performed.

PROCUREMENT

Procurement is the process of acquiring products or services from a third party. Leveraging the security department early and often can serve as a preventive control that can allow the organization to make risk-based decisions even prior to vendor or solution acceptance.

VENDOR GOVERNANCE

The goal of vendor governance is to ensure that the business is continually getting sufficient quality from its third-party providers. Professionals performing this function will often be employed at both the originating organization as well as the third-party provider.

ACQUISITIONS

Acquisitions can be disruptive to business and may impact aspects of both organizations. This is doubly true for information security.

Due diligence requires a thorough risk assessment of any acquired company's information security program, including an effective assessment of the current state of network security. This includes performing vulnerability assessment and penetration testing of the acquired company before any merger of networks.

DIVESTITURES

Divestitures (also known as demergers and deacquisitions) represent the flip side of acquisitions in that one company becomes two or more. Divestitures can represent more risk than acquisitions and pose important questions like how will sensitive data be split up? how will IT systems be split?

It is quite common for formerly unified companies to split off and inadvertently maintain duplicate accounts and passwords within the two newly spun-off companies. This allows (former) insider attacks, in which an employee of the formerly unified company hacks into a divested company by reusing old credentials. Similar risks exist with the reuse of physical security controls, including keys and badges. All forms of access for former employees must be revoked.

ETHICS

Ethics is the practice of doing what is morally right. The Hippocratic Oath, taken by doctors, is an example of a code of ethics. Ethics are of paramount concern for information security professionals: because we are often trusted with highly sensitive information, and our employers, clients, and customers must know that we will treat their information with the utmost integrity.

THE (ISC)²® CODE OF ETHICS

The (ISC)²® code of ethics is the most testable code of ethics on the exam. That's fair; you cannot become a CISSP® without agreeing to the code of ethics, among other steps, so it is reasonable to expect new CISSPs® to understand what they are agreeing to do or not do. The (ISC)²© Code of Ethics is available at the following website: http://www.isc2.org/ethics/default.aspx.

The (ISC)²® code of ethics include the preamble, canons, and guidance. The preamble is the introduction to the code. The canons are mandatory; you must follow them to become and remain a CISSP®. The guidance is "advisory," not mandatory, and it provides supporting information for the canons.

The code of ethics preamble and canons is quoted here: "Safety of the commonwealth, duty to our principals, and to each other requires that we adhere, and be seen to adhere, to the highest ethical standards of behavior. Therefore, strict adherence to this Code is a condition of certification."[1]

The (ISC)²® code of ethics canons in detail

The first and therefore most important canon of the (ISC)²® Code of Ethics requires the information security professional to "*protect society, the commonwealth, and the infrastructure*."[1] The focus of the first canon is on the public and their understanding and faith in information systems. Security professionals are charged with the promotion of safe security practices and the improvement of the security of systems and infrastructure for the public good.

The second canon in the (ISC)²® Code of Ethics charges information security professionals to "*act honorably, honestly, justly, responsibly, and legally*."[1] This canon is fairly straightforward, but there are a few points worth emphasizing here. One point that is detailed within this canon is related to laws from different jurisdictions found to be in conflict. The (ISC)²® Code of Ethics suggests that priority be given to the jurisdiction in which services are being provided. Another point made by this canon is in regard to providing prudent advice and cautioning the security professional against unnecessarily promoting fear, uncertainty, and doubt.

The (ISC)²® Code of Ethics' third canon requires that security professionals "*provide diligent and competent service to principals*."[1] The primary focus of this canon is ensuring that the security professional provides competent service for which he or she is qualified and which maintains the value and confidentiality

of information and the associated systems. An additional important consideration is to ensure that the professional does not have a conflict of interest in providing quality services.

The fourth and final canon in the (ISC)²® Code of Ethics mandates that information security professionals "*advance and protect the profession*."[1] This canon requires that the security professionals maintain their skills and advance the skills and knowledge of others. Additionally, this canon requires that individuals protect the integrity of the security profession by avoiding any association with those who might harm the profession.

DID YOU KNOW?

The (ISC)²® Code of Ethics is highly testable, including applying the canons in order. You may be asked for the "best" ethical answer, even though all answers are ethical, per the canons. In that case, choose the answer that is mentioned first in the canons. Also, the most ethical answer is usually the best, so hold yourself to a very high level of ethics for questions posed during the exam.

COMPUTER ETHICS INSTITUTE

The Computer Ethics Institute provides their *Ten Commandments of Computer Ethics* as a code of computer ethics. The code is both short and fairly straightforward. Both the name and format are reminiscent of the Ten Commandments of Judaism, Christianity, and Islam, but there is nothing overtly religious in nature about the Computer Ethics Institute's Ten Commandments. The Computer Ethics Institute's Ten Commandments of Computer Ethics are:

1. Thou shalt not use a computer to harm other people.
2. Thou shalt not interfere with other people's computer work.
3. Thou shalt not snoop around in other people's computer files.
4. Thou shalt not use a computer to steal.
5. Thou shalt not use a computer to bear false witness.
6. Thou shalt not copy or use proprietary software for which you have not paid.
7. Thou shalt not use other people's computer resources without authorization or proper compensation.
8. Thou shalt not appropriate other people's intellectual output.
9. Thou shalt think about the social consequences of the program you are writing or the system you are designing.
10. Thou shalt always use a computer in ways that ensure consideration and respect for your fellow humans.[2]

IAB'S ETHICS AND THE INTERNET

Much like the fundamental protocols of the Internet, the Internet Activities Board's (IAB) code of ethics is defined in an RFC document. RFC 1087, *Ethics and the Internet*, was published in 1987 to present a policy relating to ethical behavior

associated with the Internet. The RFC is short and easy to read, and it provides five basic ethical principles. According to the IAB, the following practices would be considered unethical behavior if someone purposely:

- Seeks to gain unauthorized access to the resources of the Internet
- Disrupts the intended use of the Internet
- Wastes resources (people, capacity, computer) through such actions
- Destroys the integrity of computer-based information
- Compromises the privacy of users.[3]

INFORMATION SECURITY GOVERNANCE

Information security governance is information security at the organizational level, which includes senior management, policies, processes, and staffing. It is also the organizational priority provided by senior leadership, which is required for a successful information security program.

SECURITY POLICY AND RELATED DOCUMENTS

Documents such as policies and procedures are a required part of any successful information security program. These documents should be grounded in reality; they are not idealistic documents that sit on shelves collecting dust. They should mirror the real world and provide guidance on the correct (and sometimes required) way of doing things.

Policy

Policies are high-level management directives. Policy is mandatory; for example, even if you do not agree with your company's sexual harassment policy, you still must follow it.

Policy is high level, and it does not delve into specifics. A server security policy would discuss protecting the confidentiality, integrity, and availability of the system, usually in those terms. It may discuss software updates and patching. The policy would not use low-level terms like "Linux" or "Windows." In fact, if you converted your servers from Windows to Linux, your server policy would not change. However, other documents, like procedures, would change.

Procedures

A procedure is a step-by-step guide for accomplishing a task. Procedures are low level and specific. Like policies, procedures are mandatory.

Here is a simple example procedure for creating a new user:

1. Receive a new-user request form and verify its completeness.
2. Verify that the user's manager has signed the form.
3. Verify that the user has read and agreed to the user account security policy.
4. Classify the user's role by following role-assignment procedure NX-103.

5. Verify that the user has selected a secret word, such as his or her mother's maiden name, and enter it into the help desk account profile.
6. Create the account and assign the proper role.
7. Assign the secret word as the initial password, and set "Force user to change password on next login to 'True.'"
8. Email the new account document to the user and their manager.

The steps of this procedure are mandatory. Security administrators do not have the option of skipping Step 1, for example, and create an account without a form.

Other safeguards depend on this procedure. For example, when a user calls the help desk as a result of a forgotten password, the help desk will follow their "forgotten password" procedure, which includes asking for the user's secret word. The help desk cannot do that unless Step 5 was completed; without that word, the help desk cannot securely reset the password. This mitigates the risks of social engineering attacks, during which an imposter tries to trick the help desk into resetting a password for an account he or she is not authorized to access.

Standards

A standard describes the specific use of technology, often applied to hardware and software. "All employees will receive an ACME Nexus-6 laptop with 8 GB of memory, a 3.3 GHZ quad core central processing unit (CPU), and 500-gigabyte disk" is an example of a hardware standard. "The laptops will run Windows 10 Enterprise, 64-bit version" is an example of a software (operating system) standard.

Standards are mandatory. Not only do they lower the TCO of a safeguard, but they also support disaster recovery.

Guidelines

Guidelines are discretionary recommendations. A guideline can be a useful piece of advice, such as "To create a strong password, take the first letter of every word in a sentence, and mix in some numbers and symbols. 'I will pass the CISSP® exam in six months!' becomes 'Iwptcei6m!'"

Baselines

Baselines are uniform ways of implementing a standard. "Harden the system by applying the Center for Internet Security Linux benchmarks" is an example of a baseline (see https://benchmarks.cisecurity.org for the Security Benchmarks division of the Center for Internet Security, a great resource). The system must meet the baseline described by those benchmarks.

Baselines are discretionary. It is acceptable to harden the system without following the aforementioned benchmarks, as long as it is at least as secure as a system hardened using the benchmarks. Formal exceptions to baselines will require senior management sign-off.

Table 1.2 summarizes the types of security documentation.

Table 1.2 Summary of Security Documentation

Document	Example	Mandatory or Discretionary?
Policy	Protect the CIA of PII by hardening the operating system	Mandatory
Procedure	Step 1: Install prehardened OS Image. Step 2: Download patches from update server. Step 3: …	Mandatory
Standard	Use Nexus-6 laptop hardware	Mandatory
Guideline	Patch installation may be automated via the use of an installer script	Discretionary
Baselines	Use the CIS Security Benchmarks Windows Benchmark	Discretionary

PERSONNEL SECURITY

Users can pose the biggest security risk to an organization. Background checks should be performed, contractors need to be securely managed, and users must be properly trained and made aware of security risks, as we will discuss next.

Security awareness and training

Security awareness and training are often confused. Awareness changes user behavior, while training provides a skill set.

Reminding users to never share accounts or write their passwords down is an example of awareness. It is assumed that some users are doing the wrong thing, and awareness is designed to change that behavior.

Security training teaches a user how to do something. Examples include training new help desk personnel to open, modify, and close service tickets; training network engineers to configure a router, or training a security administrator to create a new account.

Background checks

Organizations should conduct a thorough background check before hiring an individual. This includes a check of criminal records and verification of all experience, education, and certifications. Lying or exaggerating about education, certifications, and related credentials is one of the most common examples of dishonesty in regards to the hiring process.

Employee termination

Termination should result in immediate revocation of all employee access. Beyond account revocation, termination should be a fair process. There are ethical and legal reasons for employing fair termination, but there is also an additional information security advantage. An organization's worst enemy can be a disgruntled former employee, who, even without legitimate account access, knows where the weak spots are. This is especially true for IT personnel.

Vendor, consultant, and contractor security

Vendors, consultants, and contractors can introduce risks to an organization. They are not direct employees, and sometimes have access to systems at multiple organizations. If allowed to, they may place an organization's sensitive data on devices not controlled (or secured) by the organization.

Third-party personnel with access to sensitive data must be trained and made aware of risks, just as employees are. Background checks may also be required, depending on the level of access required. Information security policies, procedures, and other guidance should apply as well. Additional policies regarding ownership of data and intellectual property should be developed. Clear rules dictating where and when a third party may access or store data must be developed.

Outsourcing and offshoring

Outsourcing is the use of a third party to provide information technology (IT) support services that were previously performed in-house. *Offshoring* is outsourcing to another country.

Both can lower TCO by providing IT services at a reduced cost. They may also enhance the IT resources available to a company (especially a small company), which can improve confidentiality, integrity, and availability of data.

Offshoring can raise privacy and regulatory issues. For example, for a US company that offshores data to Australia, there is no HIPAA, the primary regulation covering health care data in the United States in Australia. There is no SOX (Sarbanes-Oxley, protecting publicly traded data in the United States), no Gramm-Leach-Bliley Act (GLBA, which protects financial information in the United States), etc. Always consult with legal staff before offshoring data. Contracts must ensure that data is protected, regardless of where it is located.

ACCESS CONTROL DEFENSIVE CATEGORIES AND TYPES

In order to understand and appropriately implement access controls, it is vital to understand what benefits each control can add to security. In this section, each type of access control will be defined on the basis of how it adds to the security of the system.

There are six access control types:

- Preventive
- Detective
- Corrective
- Recovery
- Deterrent
- Compensating

FAST FACTS

These access control types can fall into one of three categories: administrative, technical, or physical.

1. *Administrative* (also called directive) controls are implemented by creating and following organizational policy, procedure, or regulation. User training and awareness also fall into this category.
2. *Technical* controls are implemented using software, hardware, or firmware that restricts logical access on an IT system. Examples include firewalls, routers, encryption, etc.
3. *Physical* controls are implemented with physical devices, such as locks, fences, gates, and security guards.

PREVENTIVE

Preventive controls prevent actions from occurring. It applies restrictions to what a potential user, either authorized or unauthorized, can do. An example of an administrative preventive control is a preemployment drug screening. It is designed to prevent an organization from hiring an employee who is using illegal drugs.

DETECTIVE

Detective controls are controls that send alerts during or after a successful attack. Examples of detective controls are intrusion detection systems that send alerts after a successful attack, closed-circuit television cameras that alert guards to an intruder, and a building alarm system that is triggered by an intruder.

CORRECTIVE

Corrective controls work by "correcting" a damaged system or process. The corrective access control typically works hand in hand with detective access controls. Antivirus software has both components. First, the antivirus software runs a scan and uses its definition file to detect whether there is any software that matches its virus list. If it detects a virus, the corrective controls take over and either places the suspicious software in quarantine or deletes it from the system.

RECOVERY

After a security incident has occurred, *recovery controls* may need to be taken in order to restore the functionality of the system and organization. Recovery means that the system must be restored, which involves reinstallation from OS media or image, data restored from backups, etc.

DETERRENT

Deterrent controls deter users from performing certain actions on a system. One example is a "Beware of Dog" sign; a thief encountering two buildings, one with

guard dogs and one without, is more likely to attack the building without guard dogs. Another example is large fines for drivers who speed. A deterrent control is a sanction policy that makes users understand that they will be fired if they are caught surfing illicit or illegal websites.

COMPENSATING

A *compensating* control is an additional security control put in place to compensate for weaknesses in other controls.

RISK ANALYSIS

Accurate risk analysis is a critical skill for an information security professional. We must hold ourselves to a higher standard when judging risk. Our risk decisions will dictate which safeguards we should deploy in order to protect our assets, and the amount of money and resources we will spend doing so. Poor decisions will result in wasted money, or even worse, compromised data.

ASSETS

Assets are valuable resources that need protection. Assets can be data, systems, people, buildings, property, and so forth. The value or critical nature of the asset will dictate what safeguards you deploy.

THREATS AND VULNERABILITIES

A *threat* is a potentially harmful occurrence, like an earthquake, a power outage, or a network-based worm.

A *vulnerability* is a weakness that can allow a threat to cause harm. Examples of vulnerabilities are buildings that are not built to withstand earthquakes, a data center without proper backup power, or a Microsoft Windows 10 system that has not been patched in a long time.

RISK = THREAT × VULNERABILITY

To have risk, a threat must connect to a vulnerability. This relationship is stated by the formula:

$$\text{Risk} = \text{Threat} \times \text{Vulnerability}$$

You can assign a value to specific risks using this formula. Assign a number to both threats and vulnerabilities. We will use a range of 1–5 (the range is arbitrary; whatever range you choose to use, keep it consistent when comparing different risks).

IMPACT

The Risk = Threat × Vulnerability equation sometimes uses an added variable called *impact*: Risk = Threat × Vulnerability × Impact. Impact, or consequences, is the severity of the damage, sometimes expressed in dollars. Risk = Threat × Vulnerability × Cost is sometimes used for that reason.

EXAM WARNING

Loss of human life has a near-infinite impact on the exam. When calculating risk using the Risk = Threat × Vulnerability × Impact formula, any risk involving loss of human life is extremely high and must be mitigated.

RISK ANALYSIS MATRIX

A *risk analysis matrix*, as seen in Table 1.3,[4] uses a quadrant to map the likelihood of a risk occurring against the consequences (or impact) that risk would have.

A risk analysis matrix allows you to perform qualitative risk analysis (see section "Qualitative and Quantitative Risk Analysis") based on likelihood (from "rare" to "almost certain") and consequences or impact, from "insignificant" to "catastrophic." The resulting scores are low (L), medium (M), high (H), and extreme risk (E). Low risks are handled via normal processes; moderate risks require management notification; high risks require senior management notification; and extreme risks require immediate action including a detailed mitigation plan and senior management notification.

The goal of the matrix is to identify high likelihood/high consequence risks (upper right quadrant of Table 1.3), and drive them down to low likelihood/low consequence risks (lower left quadrant of Table 1.3).

Table 1.3 Risk Analysis Matrix

		Consequences				
		Insignificant 1	**Minor 2**	**Moderate 3**	**Major 4**	**Catastrophic 5**
Likelihood	**5. Almost Certain**	**H**	**H**	**E**	**E**	**E**
	4. Likely	**M**	**H**	**H**	**E**	**E**
	3. Possible	**L**	**M**	**H**	**E**	**E**
	2. Unlikely	**L**	**L**	**M**	**H**	**E**
	1. Rare	**L**	**L**	**M**	**H**	**H**

CALCULATING ANNUALIZED LOSS EXPECTANCY

The *annualized loss expectancy* (ALE) calculation allows you to determine the annual cost of a loss due to a risk. Once calculated, ALE allows you to make informed decisions to mitigate the risk.

This section will use an example of risk due to lost or stolen unencrypted laptops. Assume your company has 1000 laptops that contain PII. You are the security officer, and you are concerned about the risk of exposure of PII due to lost or stolen laptops. You would like to purchase and deploy a laptop encryption solution. The solution is expensive, so you need to convince management that the solution is worthwhile.

Asset value

The *asset value* (AV) is the value of the asset you are trying to protect. In this example, each laptop costs $2500, but the real value is the PII. Theft of unencrypted PII has occurred previously and has cost the company many times the value of the laptop in regulatory fines, bad publicity, legal fees, staff hours spent investigating, etc. The true average AV of a laptop with PII for this example is $25,000 ($2500 for the hardware, and $22,500 for the exposed PII).

Tangible assets, such as computers or buildings, are straightforward to calculate. Intangible assets are more challenging. For example, what is the value of brand loyalty? According to Deloitte, there are three methods for calculating the value of intangible assets: market approach, income approach, and cost approach:

- *Market approach*: This approach assumes that the fair value of an asset reflects the price at which comparable assets have been purchased in transactions under similar circumstances.
- *Income approach*: This approach is based on the premise that the value of an … asset is the present value of the future earning capacity that an asset will generate over its remaining useful life.
- *Cost approach*: This approach estimates the fair value of the asset by reference to the costs that would be incurred in order to recreate or replace the asset.[5]

Exposure factor

The *exposure factor* (EF) is the percentage of value an asset loses due to an incident. In the case of a stolen laptop with unencrypted PII, the EF is 100%, because the laptop and all of the data are gone.

Single-loss expectancy

The *single-loss expectancy* (SLE) is the cost of a single loss. SLE is the AV multiplied by the EF. In our case, SLE is $25,000 (AV) times 100% (EF), or $25,000.

Annual rate of occurrence

The *annual rate of occurrence* (ARO) is the number of losses suffered per year. For example, when looking through past events, you discover that you have suffered 11 lost or stolen laptops per year on average. Your ARO is 11.

Table 1.4 Summary of Risk Equations

	Formula	Description
Asset value (AV)	AV	Value of the asset
Exposure factor (EF)	EF	Percentage of asset value lost
Single-loss expectancy (SLE)	AV × EF	Cost of one loss
Annual rate of occurrence (ARO)	ARO	Number of losses per year
Annualized loss expectancy (ALE)	SLE × ARO	Cost of losses per year

Annualized loss expectancy

The ALE is the yearly cost due to a risk. It is calculated by multiplying SLE by the ARO. In our case, it is $25,000 (SLE) multiplied by 11 (ARO), or $275,000.

Table 1.4 summarizes the equations used to determine the ALE.

TOTAL COST OF OWNERSHIP

The TCO is the total cost of a mitigating safeguard. TCO combines upfront costs (often a one-time capital expense) plus the annual cost of maintenance, including staff hours, vendor maintenance fees, software subscriptions, etc. These ongoing costs are usually considered operational expenses.

Using our laptop encryption example, the upfront cost of laptop encryption software is $100/laptop, or $100,000 for 1000 laptops. The vendor charges a 10% annual support fee, or $10,000 per year. You estimate that it will take four staff hours per laptop to install the software, or 4000 staff hours. The staff members who will perform this work make $50 per hour plus benefits. Including benefits, the staff cost per hour is $70 multiplied by 4000 hours, which is $280,000.

Your company uses a 3-year technology refresh cycle, so you calculate the TCO over 3 years:

- Software cost: $100,000
- Three years of vendor support: $10,000 × 3 = $30,000
- Hourly staff cost: $280,000
- TCO over 3 years: $410,000
- TCO per year: $410,000/3 = $136,667 per year

Your TCO for the laptop encryption project is $136,667 per year.

RETURN ON INVESTMENT

The ROI is the amount of money saved by implementing a safeguard. If your annual TCO is less than your ALE, you have a positive ROI and have made a good choice with your safeguard implementation. If the TCO is higher than your ALE, you have made a poor choice.

Table 1.5 Annualized Loss Expectancy of Unencrypted Laptops

	Formula	Value
Asset value (AV)	AV	$25,000
Exposure factor (EF)	EF	100%
Single-loss expectancy (SLE)	AV × EF	$25,000
Annual rate of occurrence (ARO)	ARO	11
Annualized loss expectancy (ALE)	SLE × ARO	$275,000

The annual TCO of laptop encryption is $136,667; the ALE for lost or stolen unencrypted laptops is $275,000. The math is summarized in Table 1.5.

Implementing laptop encryption will change the EF. The laptop hardware is worth $2500, and the exposed PII costs an additional $22,500, for a $25,000 AV. If an unencrypted laptop is lost or stolen, the EF is 100%, because all the hardware and data are exposed. Laptop encryption mitigates the PII exposure risk, lowering the EF from 100% (the laptop and all data) to 10% (just the laptop hardware).

The lower EF lowers the ALE from $275,000 to $27,500, as shown in Table 1.6.

You will save $247,500 per year (the old ALE, $275,000, minus the new ALE, $27,500) by making an investment of $136,667. Your ROI is $110,833 per year ($247,500 minus $136,667). The laptop encryption project has a positive ROI and is a wise investment.

BUDGET AND METRICS

When combined with risk analysis, the TCO and ROI calculations factor into proper budgeting. Metrics can greatly assist the information security budgeting process. They help illustrate potentially costly risks and demonstrate the effectiveness and potential cost savings of existing controls. They can also help champion the cause of information security.

RISK CHOICES

Once we have assessed risk, we must decide what to do. Options include accepting the risk, mitigating or eliminating the risk, transferring the risk, and avoiding the risk.

Table 1.6 Annualized Loss Expectancy of Encrypted Laptops

	Formula	Value
Asset value (AV)	AV	$25,000
Exposure factor (EF)	EF	10%
Single-loss expectancy (SLE)	AV × EF	$2,500
Annual rate of occurrence (ARO)	ARO	11
Annualized loss expectancy (ALE)	SLE × ARO	$27,500

Accept the risk

Some risks may be accepted. In some cases, it is cheaper to leave an asset unprotected due to a specific risk, rather than make the effort and spend the money required to protect it. This cannot be an ignorant decision; all options must be considered before accepting the risk.

Risk acceptance criteria

Low likelihood/low consequence risks are candidates for risk acceptance. High and extreme risks cannot be accepted. There are cases where accepting the risk is not an option, such as data protected by laws or regulations and risk to human life or safety.

Mitigating risk

Mitigating risk means lowering the risk to an acceptable level. Lowering risk is also called risk reduction, and the process of lowering risk is also called reduction analysis. The laptop encryption example given in the previous ALE section is an example of mitigating the risk. The risk of lost PII due to stolen laptops was mitigated by encrypting the data on the laptops. The risk has not been eliminated entirely; a weak or exposed encryption password could expose the PII, but the risk has been reduced to an acceptable level.

In some cases, it is possible to remove specific risks entirely; this is called eliminating the risk.

Transferring risk

The insurance model depicts transferring risk. Most homeowners do not assume the risk of fire for their houses; they pay an insurance company to assume that risk for them. The insurance companies are experts in risk analysis; buying risk is their business.

Risk avoidance

A thorough risk analysis should be completed before taking on a new project. If the risk analysis discovers high or extreme risks that cannot be easily mitigated, avoiding the risk (and the project) may be the best option.

QUANTITATIVE AND QUALITATIVE RISK ANALYSIS

Quantitative and qualitative risk analysis are two methods for analyzing risk. Quantitative risk analysis uses hard metrics, such as dollar amounts, while qualitative risk analysis uses simple approximate values. Quantitative is more objective; qualitative is more subjective. *Hybrid risk analysis* combines the two by using quantitative analysis for risks that may be easily expressed in hard numbers, such as money, and qualitative analysis for the remainder.

Calculating the ALE is an example of quantitative risk analysis. The risk analysis matrix (shown previously in Table 1.3) is an example of qualitative risk analysis.

THE RISK MANAGEMENT PROCESS

The US National Institute of Standards and Technology (NIST) published *Special Publication 800-30, Risk Management Guide for Information Technology Systems* (see http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf). The guide describes a nine-step risk analysis process:

1. System Characterization
2. Threat Identification
3. Vulnerability Identification
4. Control Analysis
5. Likelihood Determination
6. Impact Analysis
7. Risk Determination
8. Control Recommendations
9. Results Documentation[6]

TYPES OF ATTACKERS

Controlling access is not limited to the control of authorized users; it also includes preventing unauthorized access. Information systems may be attacked by a variety of attackers, ranging from script kiddies to worms to militarized attacks. Attackers may use a variety of methods in their attempts to compromise the confidentiality, integrity, and availability of systems.

HACKERS

The term "hacker" is often used in the media to describe a malicious individual who attacks computer systems. The term originally described a nonmalicious explorer who used technologies in ways its creators did not intend.

While some simply use the term "hacker" to describe a malicious computer attacker, better terms include "malicious hacker," or "*black hat*." *White hat* hackers are the good guys, including professional penetration testers who break into systems with permission, or malware researchers who research malicious code to provide better understanding and ethically disclose vulnerabilities to vendors.

A *hacktivist* is a hacker activist who attacks computer systems for political reasons. "Hacktivism" is hacking activism.

Script kiddies attack computer systems with tools of which they have little or no understanding.

OUTSIDERS

Outsiders are attackers with no authorized privileged access to a system or organization. The outsider seeks to gain unauthorized access. Outsiders launch the majority of attacks, but most are usually mitigated by defense-in-depth perimeter controls.

INSIDERS

An insider attack is launched by an internal user who may be authorized to use the system that is attacked. An insider attack may be intentional or accidental. Insider attackers range from poorly trained administrators who make mistakes to malicious individuals who intentionally compromise the security of systems. An authorized insider who attacks a system may be in a position to cause significant impact.

BOTS AND BOTNETS

A *bot* (short for robot) is a computer system running malware that is controlled via a *botnet*. A botnet contains a central command and control (C&C) network, managed by humans called bot herders. The term *zombie* is sometimes used to describe a bot.

PHISHERS AND SPEAR PHISHERS

A phisher ("fisher" spelled with the hacker spelling of "ph" instead of "f") is malicious attacker who attempts to trick users into divulging account credentials or PII. Phishing is a social engineering attack that sometimes includes other attacks, including client-side attacks. Users who click links in phishing emails may be subject to client-side attacks and theft of credentials. Simply visiting a phishing site is dangerous, and the client may be automatically compromised.

SUMMARY OF EXAM OBJECTIVES

Information security governance ensures that an organization has the correct information structure, leadership, and guidance. Governance helps ensure that a company has the proper administrative controls to mitigate risk. Risk analysis helps ensure that an organization properly identifies, analyzes, and mitigates risk. Accurately assessing risk and understanding terms such as ALE, TCO, and ROI will not only help you on the exam, but also to advance your information security career.

An understanding and appreciation of legal systems, concepts, and terms are required of an information security practitioner working in the information-centric world today. The impact of the ubiquity of information systems on legal systems cannot be overstated. Whether the major legal system is civil, common, religious, or a hybrid, information systems have made a lasting impact on legal systems throughout the world, causing the creation of new laws and reinterpretation of existing laws, as well as a new appreciation for the unique aspects that computers bring to the courts.

Finally, the nature of information security and the inherent sensitivity therein makes ethical frameworks an additional point requiring attention. This chapter presented the IAB's RFC, *Ethics and the Internet*, the Computer Ethics Institute's *Ten Commandments of Computer Ethics*, and The (ISC)²® *Code of Ethics*. The CISSP® exam will, no doubt, emphasize the Code of Ethics proffered by (ISC)²®, which presents an ordered set of four canons that attend to matters of the public, the individual's behavior, the provision of competent service, and the profession as a whole.

TOP FIVE TOUGHEST QUESTIONS

Use the following scenario to answer questions 1 through 3:

Your company sells Apple iPods online and has suffered many denial-of-service (DoS) attacks. Your company makes an average $20,000 profit per week, and a typical DoS attack lowers sales by 40%. You suffer seven DoS attacks on average per year. A DoS-mitigation service is available for a subscription fee of $10,000 per month. You have tested this service and believe it will mitigate the attacks.

1. What is the ARO in the above scenario?
   - **(a)** $20,000
   - **(b)** 40%
   - **(c)** 7
   - **(d)** $10,000
2. What is the ALE of lost iPod sales due to the DoS attacks?
   - **(a)** $20,000
   - **(b)** $8000
   - **(c)** $84,000
   - **(d)** $56,000
3. Is the DoS mitigation service a good investment?
   - **(a)** Yes, it will pay for itself.
   - **(b)** Yes, $10,000 is less than the $56,000 ALE.
   - **(c)** No, the annual TCO is higher than the ALE.
   - **(d)** No, the annual TCO is lower than the ALE.

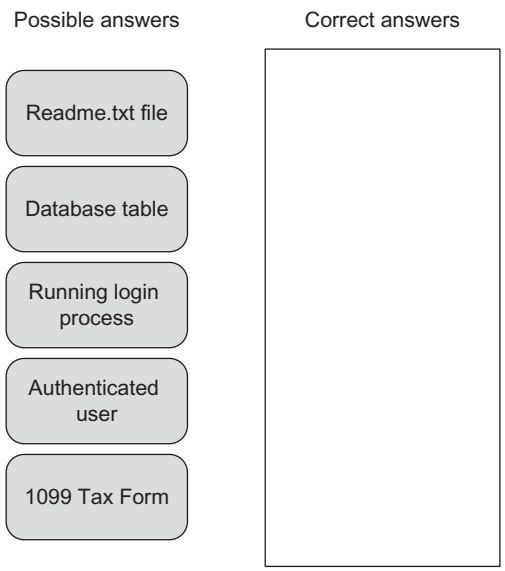

FIG. 1.5

Drag and drop.

4. Which canon of The (ISC)2® Code of Ethics should be considered the most important?
   (a) Protect society, the commonwealth, and the infrastructure
   (b) Advance and protect the profession
   (c) Act honorably, honestly, justly, responsibly, and legally
   (d) Provide diligent and competent service to principals
5. *Drag and drop*: Identify from the list below items that can be classified as objects. Drag and drop the objects from left to right (Fig. 1.5).

ANSWERS

1. Correct answer and explanation: C. The ARO is the number of attacks in a year.
   Incorrect answers and explanations: Answers A, B, and D are incorrect. The AV is $20,000. The EV is 40% and the monthly cost of the DoS service (used to calculate TCO) is $10,000.
2. Correct answer and explanation: D. The ALE is derived by first calculating the SLE, which is the AV, $20,000, multiplied by the EF, 40%. The SLE is $8000, which is multiplied by the ARO of 7 for an ALE of $56,000.
   Incorrect answers and explanations: Answers A, B, and C are incorrect. $20,000 is the AV, while $8000 is the SLE.
3. Correct answer and explanation: C. The TCO of the DoS mitigation service is higher than ALE of lost sales due to DoS attacks. This means it is less expensive to accept the risk of DoS attacks or to find a less expensive mitigation strategy.
   Incorrect answers and explanations: Answers A, B, and D are incorrect. The annual TCO is higher, not lower. $10,000 is the monthly TCO; you must calculate yearly TCO to compare with the ALE.
4. Correct answer and explanation: A. The canons are applied in order and "To protect society, the commonwealth, and the infrastructure" is the first canon, and is thus the most important of the four canons of The (ISC)²® Code of Ethics.
   Incorrect answers and explanations: Answers B, C, and D are incorrect. The canons of The (ISC)²® Code of Ethics are presented in order of importance. The second canon requires the security professional to act honorably, honestly, justly, responsibly, and legally. The third mandates that professionals provide diligent and competent service to principals. The final and therefore least important canon wants professionals to advance and protect the profession.
5. Correct answer and explanation: Files, database tables, and tax forms are example of objects, so they should be dragged to the right (Fig. 1.6).
   Incorrect answers and explanations: A running process and a user are examples of subjects.

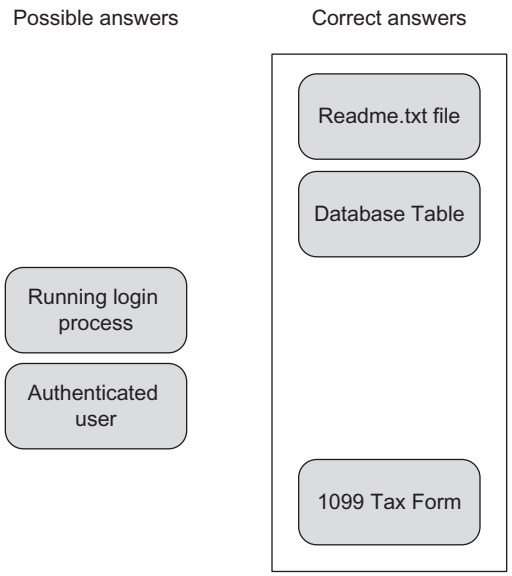

FIG. 1.6

Drag and drop answer.

ENDNOTES

1. *(ISC)²® Code of Ethics*. Available from http://www.isc2.org/ethics/default.aspx [accessed 25.04.16].
2. *Computer Ethics Institute. Ten Commandments of Computer Ethics*. Available from http://computerethicsinstitute.org/publications/tencommandments.html; 1992 [accessed 25.04.16].
3. *Internet Activities Board. RFC 1087—Ethics and the Internet*. Available from http://tools.ietf.org/html/rfc1087; 1989 [accessed 25.04.16].
4. *National Museum of Australia Collection Care and Preservation Policy*. Available from http://www.nma.gov.au/about_us/ips/policies/collection_care_and_preservation_policy [accessed 25.04.16].
5. *Intangible Assets—Recognising their Value*. http://www2.deloitte.com/content/dam/Deloitte/ie/Documents/Finance/Corporate%20Finance/2009_valuing_intangible_assets_deloitte_ireland.pdf [accessed 25.04.16].
6. *Risk Management Guide for Information Technology Systems*. http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf [accessed 25.04.16].